RECEIVED
CENTRAL FAX CENTER
AUG 18 2005

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission: 14

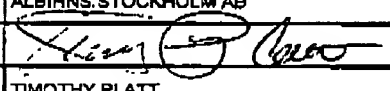
Application Number	09/423,511
Filing Date	11/10/1999
First Named Inventor	HANS SJOBLOM
Art Unit	3621
Examiner Name	CHEUNG, MARY DA ZHI WANG
Attorney Docket Number	70324-BB523

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☑ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please identify below):

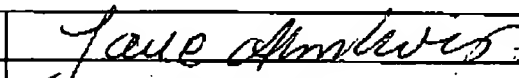
Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	ALBIHNS STOCKHOLM AB		
Signature			
Printed name	TIMOTHY PLATT		
Date	2005-08-18	Reg. No.	43,003

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Jane Almkvist	Date	2005-08-18

RECEIVED
CENTRAL FAX CENTER
AUG 18 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re. Patent Application of
Hans SJÖBLOM
Application No. 09/423511
§371(c) date: 10 November 1999

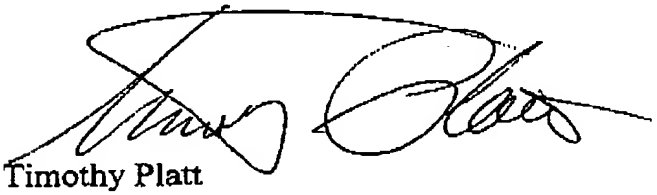
Group Art Unit: 3621
Examiner: Cheung, M.

For: Method and Device for Performing Electronic Transactions

An amended appeal brief to conform with the new rules concerning format and content of the appeal brief is submitted herewith.

If no new Examiner's Answer is issued, it is requested that the Reply Brief of 21 march 2005 stand as submitted.

Respectfully submitted,



Timothy Platt
Reg. No. 43,003
18 August 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re. Patent Application of
Hans SJÖBLOM
Application No. 09/423511
§371(c) date: 10 November 1999

Group Art Unit: 3621
Examiner: Cheung, M.

For: Method and Device for Performing Electronic Transactions

Amended Brief in Support of Appeal

Real Party in Interest

The subject application is owned by Comex Electronics AB of Täby, Sweden.

Related Appeals and Interferences

To the knowledge of the appellant, the assignee or his agent, no other appeal or interference will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

On 22 October 2004, appealed from the decision dated 22 March 2004 of the examiner finally rejecting Claims 1-29, Claims 3 and 4 having been cancelled, Claims 1, 3, 6-13, 15, 17-19 having been amended and Claims 27-29 having been added during prosecution.

Status of Amendments

Subsequent to the final rejection of 22 March 2004, the appellant filed an amendment to Claim 1 specifying that the electronic transactions are performed

"via a communications network". Also Claims 4 and 5 were deleted as being redundant. In the Advisory Action of 22 September 2004, it was indicated that these amendments were entered, but without further comment than that "the arguments are not persuasive".

Summary of Claimed Subject Matter

Claim 1-20 and 27-29 in force relate to a method for performing electronic transactions via a communications network using a smart card. (See the entire description.) Claims 21 and 22 relate to a smart card for carrying out electronic transactions. (See page 7, lines 7- 21; page 9, lines 25-31). Claims 23-25 relate to a combination of a smart card and a user-controlled communication unit. (See page 7, lines 22-35). Claim 26 relates to the use of a smart card. (See the entire description.)

In order to preserve absolute, physical, integrity when formulating the encrypted transaction message to be sent, creates, using software previously stored in the smart card, the transaction message in the smart card, independently of any connection to a communications network and without computer dialogue, before digitally signing it in the smart card. The central concept of the invention is the elimination of any possibility that any second of third party or their computer will compromise the integrity of the transaction message at any time during the process of its being created and electronically signed and sealed by the sender. (See pages 2-8 , and in particular page 5, last paragraph and page 6 first paragraph.)

Grounds of Rejection to be Reviewed on Appeal

Against Claims 1-9, 11-13, 15-18, 21-23 and 25-29 in this application, US Patent 6 038 551 (*Barlow et al.*) has been cited under §102 in the final rejection of 22 march 2004. Under §103, Claim 14 was rejected citing *Barlow et al* and

Claims 10, 19-20 and 24 were rejected over *Barlow et al.* in view of *Heinonen et al.* (US 5,887,266).

The Examiner's Rationale

The Examiner's reasoning in rejection of the claims citing *Barlow et al* is inter alia that: *Barlow et al* does in fact teach the creation of a transaction message on the basis of entered transaction information in the smart card with the aid of software previously stored in the smart card. Barlow teaches this matter, in particular at column 14 lines 62 – column 15 line 10; Barlow teaches a user selecting beverage which corresponds to creating a transaction message, and the IC card are used for this beverage transaction which corresponds to the usage of the smart card as claimed, states the Examiner.

The Examiner also takes up one feature of the claimed invention, namely lack of interaction with a communications network during the creation of the message. The Examiner states that "the vending machine purchase in Barlow's teaching (column 14 lines 62 – column 15 line 10) corresponds to this limitation because Barlow explicitly states "the vending machine is an example of an offline computer".

Argument

§102 against Claims 1-9, 11-13, 15-18, 21-23 and 25-29.

Barlow et al. describes a user-configurable smartcard, which can be used in a plurality of different systems. Of those systems discussed in *Barlow et al.*, three of them [a. ATM cash withdrawal (col. 14, lines 42-58), b. vending machine purchases (col. 14, line 62 – col. 15, line 10) and c. on-line shopping (col. 15 and 16)] can be characterized as financial transaction systems.

a. ATM cash withdrawal (col. 14, lines 42-58). This example in *Barlow et al.* illustrates how a financial transaction is effected using a smart card and an automatic teller machine. Lines 48-52 read: "Next, the IC card and the banking application running on the ATM exchange authentication information. The banking application then conducts a financial transaction through the API to the IC card." It is submitted that this describes prior art methods where there is **back-and-forth** interaction between the sender and the receiver [the bank's computer] during the creation of the transaction method and prior to its being electronically signed by the sender. Typically, conducting a financial transaction through the API [Application Program Interface] to the IC card involves back and forth communication with a computer outside the sender's complete control. This is illustrated by the flow chart shown in Figs. 7-10 of *Barlow et al.* where steps 158-162, steps 170-174 and steps 180-186 all involve back and forth interaction with a second or third party computer **during** the creation of the signed transaction message. This is contrary to the concept of the invention as defined in the pending main claim.

b. Vending machine purchases (col. 14, line 62 – col. 15, line 10). The cited passage in *Barlow et al.* refers to a known cash card which has a chip "loaded" with a certain amount of money. During use in a vending machine, the vending machine is able to interact with the chip and electronically deduct a certain payment amount from the chip on the cash card leaving the remaining amount in the chip for future purchases until completely used up and/or reloaded with money. There are significant difference between this known technology and the method for performing electronic transactions as disclosed in Claim 1. The present invention creates a "transaction message" "in the smart card with the aid of software previously stored in the smart

card". Also the created transaction message is provided with the senders "digital signature while using his own private key for subsequent output and transmission of the transaction message." While it is true that the above described use according to *Barlow et al.* of a cash card in a vending machine completes a transaction off-line, no digitally signed transaction message is produced and transmitted. Only an electronic deduction is made in the chip on the card by a mechanism in the vending machine. No message is ever digitally signed and transmitted in the vending machine example from *Barlow et al.* cited against Claim 1. Digitally signing and transmitting a message is the very purpose of the present invention, that is to say creating and digitally signing a complete coded transaction message in the card without any possibility whatsoever of so-called hacking, and then transmitting the message to a receiver via a communications network.

c. On-line shopping (col. 15 and 16). The entire described purchase process involves continual **back-and-forth** exchange of information: "Authentication information is exchanged between the IC card and shopping application for mutual verification." (col. 15, lines 27-28) ; "... mutually authenticated each other through the exchange of certificates. When the user is ready to place an order, the user and merchant computers will first exchange certificates." (col. 16, lines 13-16); "The user's computer and the merchant's computing unit then exchange the certificates over the public network (step 158). Upon receipt of the merchant's certificate, the commerce application submits the merchant's certificate through the card management and cryptography API 36 to the IC card 14 (step 160). the card processor 50 examines the signature on the certificate to verify that it belongs to the certifying authority in this context (step 162). If the certificate is

valid , the merchant identifying information can be checked and the public keys used to authenticate the merchant using a challenge response protocol. "

All of the examples in *Barlow et al.*, involve interaction, before completion of the digitally signed message, with entities outside the sender's control, in particular in this case entities outside the actual smart card itself. Nowhere in *Barlow et al.* is there any indication of the concept of the present invention. All that *Barlow et al.* reveals is the previously known interacting technology which opens the possibility of hacking, intrusion and errors during the compiling and digital signing of the transaction message. It is submitted that the independent claims 1, 21 and 23 are new and non-obvious over *Barlow et al.*

§103 against Clams 10, 19-20 and 24.

US Patent 6 038 551 to *Heinonen et al* . cited in combination with *Barlow et al.* against Claims 10, 19-20 and 24 which are dependent claims, which in combination with an allowable independent claim do not need to exhibit novelty and non-obviousness in themselves. Nonetheless, *Heinonen et al.* only discloses the use of a mobile phone in a financial transaction conducted in the standard previously known manner, i.e. with back and forth interaction with an outside party during the formulation of the transaction message, i.e. offering a physical possibility of interference, reducing the sender's absolute confidence in the integrity of the transaction message, which is the purpose of the present invention. It is therefore maintained that all of the claims are allowable even over *Barlow et al.* in view of *Heinonen et al.*

Claims Appendix

A copy of the pending claims is appended herewith.

Evidence Appendix

No new evidence

Related Proceedings Appendix

Not applicable

~~Respectfully submitted,~~

Timothy Platt
Reg. No. 43,003
18 August 2005

Albihns Stockholm AB
Box 5581
114 85 Stockholm, Sweden

CLAIMS

1.(amended) A method for performing electronic transactions via a communications network, in which a sender of transaction messages is assigned a smart card with an associated unique identity and a private key stored in the card in a protected manner, and in which an associated public key is kept generally available,
c h a r a c t e r i s e d in that in connection with an electronic transaction under the sender's own control, preferably through his own input of message information, the sender, independently of any connection to a communications network and without computer dialogue with a receiver, creates, on the basis of entered transaction information, a transaction message, which contains information necessary for the transaction, the transaction message being created in the smart card with the aid of software previously stored in the smart card, and, in his smart card, provides the created transaction message with his digital signature while using his own private key for subsequent output and transmission of the transaction message.

2.(Original) A method as claimed in claim l, c h a r a c t e r i s e d in that the transaction message contains information on sender, receiver, amount and preferably a transaction serial number.

3.(Previously amended) A method as claimed in claim 1 c h a r a c t e r i s e d in that the transaction message is created off-line, i.e. not connected to the communications network that is used for the subsequent transmission of the transaction message.

4.(Deleted) .

5.(Deleted) .

6. (Previously amended) A method as claimed in claim 5, c h a r a c t e r i s e d in that the transaction message is created with the aid of sender information inserted in the card in advance.

7. (Previously amended) A method as claimed in claim 5, c h a r a c t e r i s e d in that information required for the transaction message is input with the aid of input means arranged on the smart card, the card preferably being a so-called advanced smart card.

8. (Previously amended) A method as claimed in claim 1, characterised in that information necessary for the transaction message is input with the aid of a protected card terminal.

9. (Previously amended) A method as claimed in claim 1, characterised in that information necessary for the transaction message is input with the aid of a separate card communication unit, the latter preferably also being a card activator.

10. (Previously amended) A method as claimed in claim 1, characterised in that information necessary for the transaction message is input with the aid of a telecommunications unit controlled by the smart card, especially a mobile telecommunications unit such as a mobile phone.

11. (Previously amended) A method as claimed in claim 1,characterised in that the transaction message contains sender information in the form of at least one of the following pieces of information: a card number, a cash card number, a charge card number, a credit card number, an account number, an invoice number and an ID number.

12. (Previously amended) A method as claimed in claim 1, characterised in that the transaction message contains receiver information in the form of at least one of the following pieces of information: a card number, a cash card number, a charge card number, a credit card number, an account number, an invoice number and an ID number.

13. (Previously amended) A method as claimed in claim 1, characterised in that the signed transaction message is sent to a card or account administrator regarding the sender or receiver, that the digital signature of the transaction message is authenticated by using the public key, which is assigned to the one who is identified as sender by the transmitted transaction message, and that in case of authenticity, the receiver is credited with the transaction amount by a clearing process.

14.(Original) A method as claimed in claim 13, characterised in that the signed transaction message isfirst sent to the receiver, who optionally after his own checking of the digital signature of the message forwards the signed transaction message to said card or account administrator.

15. (Previously amended) A method as claimed in claim 1, c h a r a c t e r i s e d in that the signed transaction message is encrypted by using a public key belonging to the addressee, to whom the transaction message is sent, that the encrypted, signed transaction message is sent to the addressee, that the addressee by using his private key decrypts the signed transaction message, that the digital signature of the transaction message is authenticated by using the public key which is assigned to the one who is identified as sender by the transmitted transaction message, and that the receiver, in case of authenticity, is credited with the transaction amount by a clearing process.

16.(Original) A method as claimed in claim 15, c h a r a c - t e r i s e d in that the addressee is the receiver, that the receiver, after decryption, sends the signed transaction message to a card or account administrator, whereupon said authentication takes place.

17. (Previously amended) A method as claimed in claim 1, c h a r a c t e r i s e d in that the signed transaction message is encrypted by using the sender's public key and is provided with sender information and is then sent to a card or account administrator, who has the sender's private key and who preferably has issued the user's smart card, that said administrator decrypts the received encrypted message by using said private key, that authentication of the digital signature of the decrypted transaction message takes place by using the public key, which is assigned to the one who is identified as sender by the transmitted transaction message, and that the receiver, in case of authenticity, is credited with the transaction amount by a clearing process.

18. (Previously amended) A method as claimed in claim 1, c h a r a c t e r i s e d in that the signed transaction message is sent non-encrypted, especially via a public communications network, such as the Internet or a telecommunications network.

19. (Previously amended) A method as claimed in claim 1, c h a r a c t e r i s e d, in that the signed transaction message is sent by e-mail.

20.(Original) A method as claimed in any one of claims 1-18, c h a r a c t e r i s e d in that the signed transaction message is sent via a mobile telephone network, especially by using a so-called SMS service.

21.(Original) A smart card for carrying out electronic transactions, comprising means for storing card identification information, means for protected storing of a

private key, means for storing an asymmetrical algorithm, means for input of transaction information into the card, processor means for creating in the card a transaction message based on input transaction information, such as information on amount and receiver, and optionally information stored in the card, such as information on sender and preferably a serial number, and for providing the transaction message with a digital signature on the basis of said private key and said asymmetrical algorithm, and means for output of the signed transaction message.

22. (Previously amended) A card as claimed in claim 21, c h a r a c t e r i s e d in that the card is of a so-called advanced type.

23.(Original) A combination of a smart card and a user-controlled communication unit, which is arranged for communication with the smart card and with which the card is adapted to be combined with a view to producing an electronic transaction message, the card comprising means for protected storing of a private key, means for storing an asymmetrical algorithm and processor means for providing a created transaction message with a digital signature based on said private key and said algorithm, and said communication unit comprising means for input of transaction information, and means being arranged in the communication unit and/or in the card for creating said transaction message.

24.(Original) A combination as claimed in claim 23, c h a r a c t e r i s e d in that the communication unit is a mobile telecommunication device.

25.(Original) A combination as claimed in claim 23, c h a r a c t e r i s e d in that the communication unit is a combined card activator and information inputter/processor.

26.(Original) Use of a smart card with a private key stored therein for providing, independently of the communications network, an electronic transaction message provided with a digital signature based on the private key.

27.(Previously added) A method as claimed in claim 2, c h a r a c t e r i s e d in that the transaction message is created off-line, i.e. not connected to the communications network that is issued for the subsequent transmission of the transaction message.

28.(Previously added) A method as claimed in claim 6, c h a r a c t e r i s e d in that information required for the transaction message is input with the aid of input means

arranged on the smart card, the card preferably being a so-called advanced smart card.

29.(Previously added) A method as claimed in claim 27, c h a r a c t e r i s e d in that the transaction message is created off-line.